RESEARCH ARTICLE OPEN ACCESS

# Bitcoin and Ethereum: Examples of Distributed Computing Applications

**Shamsudeen E**

Assistant Professor of Computer Applications
EMEA College of Arts and Science, Kondotty, Kerala – India

**ABSTRACT**
Bitcoin and Ethereum are very good distributed computing applications which actually rule the world of cryptocurrency market today. Bitcoin signaled the emergence of a radically new form of digital money that operates outside the control of any government or corporation.With time, people began to realize that one of the underlying innovations of bitcoin, the blockchain, could be utilized for other purposes. Ethereum proposed to utilize blockchain technology not only for maintaining a decentralized payment network but also for storing computer code which can be used to power tamper-proof decentralized financial contracts and applications. The blockchain technology is a relatively new approach in the field of information technologies. Ethereum applications and contracts are powered by ether, the Ethereum network's currency.Ether was intended to complement rather than compete with bitcoin, but it has nonetheless emerged as a competitor on cryptocurrency exchanges.
As one of its first implementations, bitcoin as a cryptocurrency has gained a lot of attention. Together with Ethereum, blockchain implementation with focus on smart contracts, they represent the very core of modern cryptocurrency development. This article is meant to give a brief introduction to these topics

***Kerywords*: Distributed computing, bitcoin, ethereum, blockchain

## I. INTRODUCTION

One of the most critical issues in today's world of virtual networks is privacy. It's possible that you recently may have heard this term more frequently than ever. Distributed computing provides the answer for all these privacy problems.
A distributed system[1] in its most simplest definition is a group of computers working together as to appear as a single computer to the end-user. These machines have a shared state, operate concurrently and can fail independently without affecting the whole system's uptime. That is a distributed system is with multiple components located on different machines that communicate and coordinate actions in order to appear as a single coherent system to the end-user. It does not reveal the existence of multiples systems.
With the ever-scaling technological expansion of the world, distributed systems are becoming more and more used and has significance. They are a sophisticated field of study in computer science and applications.
The machines that are a part of a distributed system may be computers, physical servers, virtual machines, containers, or any other node that can connect to the network, have local memory, and communicate by passing messages.
Application that can make use of the capabilities offered by a distributed computing system is called a distributed application(DApp)[2]. The execution and structure of such an application's back end needs to be carefully designed in order to be compatible with the system.

The blockchain[3] presents an opportunity to store data in a distributed system of participating nodes. Stepping up from this opportunity we can logically build systems and applications running on such a network Ethereum[4], being a distributed public blockchain network run by nodes instead of clouds or servers, aims to build a more democratized and more secure environment to the existing client-server models.
Bitcoin[5] to be one among a list of applications of distributed computing. The point is that any cryptocurrency currently running on a blockchain backbone can be termed as a DApp. Cryptocurrencies are in fact the most popular DApp format out there and a revolutionary one.

### *I.1. Working principle of a distributed system*

There are two general ways that distributed systems function:

I. Each machine works toward a common goal and the end-user views results as one cohesive unit.
II. Each machine has its own end-user and the distributed system facilitates sharing resources or communication services.

## II. TYPES OF DISTRIBUTED SYSTEMS

Distributed systems are generally classified into four basic categories based on their architecture.

*2.1. Client-server*
Clients sends the request to the server to get some service from the server site. Client acts as a requester and sever acts as a master as it fulfills the requests of the client.

*2.2. Three-tier*
Information about the client is stored in a middle tier rather than on the client site to simplify application deployment. This architecture model is most common for web applications.

*2.3. n-tier*
Generally used when an application or forward requests to additional enterprise services on the network.

*2.4. Peer-to-peer*
Here all the systems gets the equal priority. Responsibilities are uniformly distributed among machines in the system, known as peers, which can serve as either client or server.

## III. DISTRIBUTED APPLICATIONS

These are applications where more than one servers behind a single load balancer and all are connected to one database. Such applications are , Bitcoin and Ethereum. A system is distributed only if the nodes communicate with each other to coordinate their action and make the user the feelings of a single coherent system.

### *3.1. Ethereum*

Launched in July of 2015, Ethereum is the largest and most well-established, open-ended decentralized software platform[6].

Ethereum enables the deployment of smart contracts and decentralized applications to be built and run without any downtime, fraud, control or interference from a third party.A smart contract is pretty much exactly what you think it would be: it's an auto-executing, programmed agreement that is recorded on the Ethereum blockchain. It operates based upon an *if, then* logic, so that if x action happens, then y action occurs. Ethereum comes complete with its own programming language which runs on a blockchain, enabling developers to build and run distributed applications.

Four core technological building blocks form the foundation of Ethereum's smart contract[7] platform are,

#### *3.1.1.Cryptographic tokens and addresses*

A mathematically secure unique voucher system that allows for assets to be built on existing blockchains. These act as a standard for computing value, or numeraire. They can serve as payment for goods, services, and can also be used to represent a mathematically secured and pseudonymous identity.

#### *3.1.2. Peer-to-peer networking*

Individual users connect their computers together to form a network that can exchange data without a central server. Bitcoin and Ethereum run on Peer-to-Peer networks[8], as does nearly every other cryptocurrency in use today.

#### *3.1.3. Consensus algorithms*

These algorithms permit blockchain users to reach a consensus about the current state of the blockchain. The Bitcoin blockchain reaches consensus on a global state change (which typically involves adding a new block to the blockchain) about once every 10 minutes, whereas the Ethereum blockchain reaches consensus in approximately 15 seconds.

#### *3.1.4. Turing complete virtual machine*

A virtual machine[9] is a computer that exists in software form and can be run at a layer of abstraction above its underlying hardware. A "Turing complete" system can run any program and is powerful enough to implement any program defined in any similarly computationally complete system. For comparison, Bitcoin is not Turing-complete as its virtual machine can only run a much simpler class of programs.

These four pillars of dapp technology are designed to enable smart contracts. Smart contracts usually have a user interface that can be implemented as a web page, an application, or a mobile app. In the future, traditional contracts may become outdated for the purposes of certain transactions. Rather than drafting a costly, lengthy contract employing attorneys, banks, notaries, and Microsoft Word, contracts could be created with a few lines of code. Smart contracts could potentially be constructed automatically by wiring together a handful of human-readable clauses.

The potential applications of Ethereum are wide-ranging and are powered by its native cryptographic[10] token, ether (ETH). Ether is like the fuel for running commands on the Ethereum platform and is used by developers to build and run applications on the platform.

Ether is used mainly for two purposes—it is traded as a digital currency on exchanges in the same fashion as other cryptocurrencies, and it is used on the Ethereum network to run applications. According to Ethereum, people all over the world use ETH to make payments, as a store of value, or as collateral.

### *3.2. Bitcoin*

Bitcoin was launched in January of 2009. It introduced a novel idea set out in a white paper by the mysterious Satoshi Nakamoto—bitcoin offers the promise of an online currency that is secured without any central authority, unlike government-issued currencies. There are no physical bitcoins, only balances associated with a cryptographically secured public ledger. Although bitcoin was not the first attempts at an online currency of this type, it was the most successful in its early efforts, and it has come to be known as a predecessor in some way to virtually all cryptocurrencies which have been developed over the past decade.

#### *3.2.1. Consensus in the distributed system leads to Bitcoin*

Consensus[11] is the problem in distributed systems of getting members of a network to agree on something, e.g. a value. In some systems, there is a centralized control unit who can decide on the value and then broadcast it to the rest of a network. In a distributed consensus system, members of the group have to collectively reach consensus without the benefit of a centralized unit. Further complicating the problem, some members of the group of the distributed system may be lying or otherwise manipulating the group to try and reach a consensus that favors them over the true value.

There are various solutions to the problem of distributed consensus. In the approach used by Bitcoin, a distributed currency with no central bank or other authority, can solve the problem of consensus. To work with a distributed currency properly members of the network must agree on how many units of the currency each member holds at all times, in order to prevent members from double spending, i.e. re-using the same units of currency in multiple transactions. That is the distributed consensus problem.

Bitcoin uses mining to reach a consensus in the transactions. Members of the network who choose to take part in the process of reaching a distributed consensus are called miners. Mining involves forming a block containing a series of transaction records, then finding a valid proof of work for that block that satisfies certain rules. Specifically, miners increment a nonce until they find a value that gives the block's hash a certain number of leading zeros, thereby finding the next block in the blockchain.

These Bitcoin miners[12] run complex computer rigs to solve complicated puzzles in an effort to confirm groups of transactions called blocks; upon success, these blocks are added to the blockchain record and the miners are rewarded with a small number of bitcoins. Interestingly, other participants in the Bitcoin market can buy or sell tokens through cryptocurrency exchanges or peer-to-peer. However,the Bitcoin ledger is protected against fraud via a trustless system; Bitcoin exchanges also work to defend themselves against potential theft, but high-profile thefts have occurred. The interesting thing is that nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

The previous distributed payment protocols was not able to prevent the double-spending problem in real time, in a distributed manner. But the Bitcoin technology solved this double spending issue first time by implementing a practical solution with clear advantages over others.

The double spending problem states that an actor (e.g Khan) cannot spend his single resource in two places. If Khan has Rs. 100, he should not be able to give it to both Priyanka and Karishma — it is only one asset, it cannot be duplicated. It turns out it is really hard to truly achieve this guarantee in a distributed system. There are some interesting mitigation approaches predating blockchain, but they do not completely solve the problem in a practical way.

Double-spending is solved easily by Bitcoin, as only one block is added to the chain at a time. Double-spending is impossible within a single block, therefore even if two blocks are created at the same time — only one will come to be on the eventual longest chain.

## IV. KEY DIFFERENCES

Though both the Bitcoin and Ethereum networks are powered by the principle of distributed ledgers and cryptography, in many ways the two differ technically . For example, transactions on the Ethereum network may contain executable code, while data affixed to Bitcoin network transactions are generally only for keeping notes. The second difference is that the block time -an ether transaction is confirmed in seconds compared to minutes for bitcoin. The third difference is that the algorithms that they run on -Ethereum uses ethash while Bitcoin uses SHA-256.

Moreover, the Bitcoin and Ethereum networks are different with respect to their overall aims. While bitcoin was created as an alternative to national currencies and thus aspires to be a medium of exchange and a store of value, Ethereum was intended as a platform to facilitate immutable, programmatic contracts, and applications via its own currency.

BTC and ETH are both digital currencies, but the primary purpose of ether is not to establish itself as an alternative monetary system, but rather to facilitate and monetize the operation of the Ethereum smart contract and decentralized application platform.

Ethereum is another use-case for a blockchain that supports the Bitcoin network, and theoretically should not really compete with Bitcoin. However, the popularity of ether has pushed it into competition with all cryptocurrencies, especially from the perspective of traders. For most of its history since the mid-2015 launch, by market cap ether has been close behind bitcoin on rankings of the top cryptocurrencies .

## V. FUTURE SCOPE OF CRYPTOCURRENCY

The cryptocurrency industry has potential to shape our collective future. It is ultimately about the move away from a centralized system for organizing society towards a decentralized one that is more appropriate for the technological present. Indeed, the question of centralization versus decentralization is central to the framework of blockchain technology. For all of recorded history, human beings have achieved scale through a bureaucracy. Empires, nation states, and corporations are all built upon layers of authority and thickets of bureaucracy. Blockchain manages to overcome this by shifting the burden of validation from the center to the periphery. In other words, no central authority is required in order to approve any transaction or mediate any dispute among users of the blockchain protocol. There is no need for third-party verification.

## VI. CONCLUSION

In this article, it is managed to define what a distributed system is and how bitcoin is managed to solve the double spending issue of distributed computing. Both Bitcoin and Ethereum offers a distributed blockchain network. Although there are significant differences between these two, the most crucial distinction is their purpose and capability. Bitcoin enables its users to send peer to peer electronic payment which is leveraged in many application domains. Ethereum, on the other hand, supports many different use cases where decentralization is sustained by smart contracts.

Ethereum was developed to augment and improve on bitcoin, expanding its capabilities. Importantly, it was developed to feature prominently smart contracts: decentralized, self-executing agreements coded into the blockchain itself. Its blockchain is built with a turing-complete scripting language that can simultaneously run such smart contracts across all nodes and achieve verifiable consensus without the need for a trusted third party such as a court, judge or legal system.

## REFERENCES

1. Waldo, J., Wyant, G., Wollrath, A. and Kendall, S. (1994). A note on distributed computing. In Arnold et al. 1999
2. Rellermeyer, J. S., Alonso, G., and Roscoe, T. (2007). R-OSGi: Distributed applications through software modularization. In Proceedings of the ACM/IFIP/USENIX 2007 international Conference on Middleware, Newport Beach, CA, November.
3. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016
4. V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resourse sharing," 1st Workshop on Economics of Peer-To-Peer Systems, 2003
5. Bitcoin Blockchain Size, https://charts.bitcoin.com/chart/blockchain-size
6. Ethereum Community, "A next-generation smart contract and decentralized application platform," White Paper, available at: https://github.com/ethereum/wiki/wiki/White-Paper
7. V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," 2013, available at: http://www.the-blockchain.com/docs/Ethereum_white_paper_next_generation_smart_contract_and_decentralized_application_platf orm-vitalik-buterin.pdf
8. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, available at: https://bitcoin.org/bitcoin.pdf
9. Whitaker, A., Shaw, M. and Gribble, D.G. (2002). Denali: Lightweight virtual machines for distributed and networked applications . Technical Report 02-02-01, University of Washington.
10. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," Financial Cryptography, 2015
11. Back, "Hashcash – a denial of service counter-measure," 2002, available at: http://www.hashcash.org/papers/hashcash.pdf
12. A. Hertig, "SegWit goes live: why Bitcoin's big upgrade is a blockchain game-changer," August 2017, available at: https://www.coindesk.com/50-blocks-segwit-bitcoins-coming-upgrade-blockchain-game-changer/